

# Global Information Grid Bandwidth Expansion (GIG-BE)

## Executive Summary

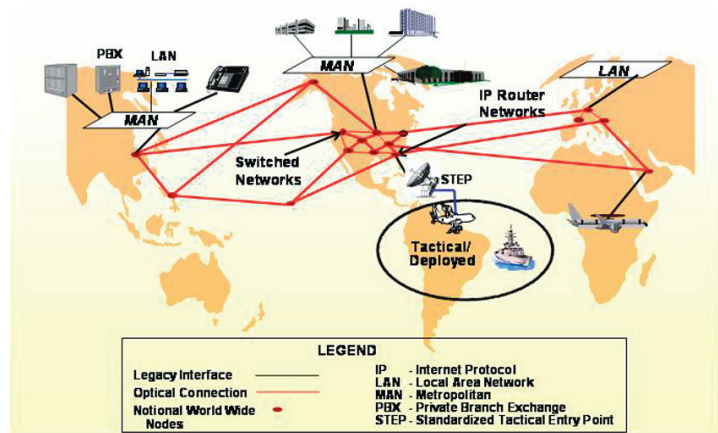
- The Joint Interoperability Test Command (JITC) conducted a series of operational assessments in 2005, and a full-capability operational test and evaluation from September 19, 2005, to October 7, 2005. The evaluations of all these events contribute to the Full Operational Capability (FOC) decision in November 2005.
- Based on the IOT&E in September 2004 and the operational assessments in 2005, the network and its supporting management processes are effective for the near-term level of traffic and user population. Operational suitability and survivability will be assessed at the end of full-capability operational test and evaluation. Data is currently under analysis by the test team.
- Because the Global Information Grid Bandwidth Expansion (GIG-BE) will become the backbone of most DoD and intelligence community systems, DOT&E believes additional evaluation will be needed in the areas of information assurance, configuration management, the fully implemented Secret and Top Secret/Sensitive Compartmented Information (TS/SCI) network, and survivability to support the Global Information Grid.

## System

- GIG-BE is a key enabler of DoD's transformation to net-centric operations.
- GIG-BE is a government-owned, ground-based, backbone-switched communications network. It connects 88 major DoD sites throughout the continental United States, Europe, and the Pacific theater.
- The communications backbone consists of high-capacity fiber optical links with up to 80 channels of 10 Gigabits each.
- GIG-BE is government designed using commercially developed components. Component and network integration tests were performed by commercial contractors in commercial laboratories.

## Activity

- An IOT&E follow-on operational assessment performed in January 2005 and another operational assessment in May, addressed many of the open issues from the September 2004 IOT&E.
- Security Test and Evaluation of the unclassified, Secret, and TS/SCI networks supported approval of a three-year Authority to Operate. A JITC information assurance group review, conducted separately, identified additional concerns.
- Beginning in July 2005, operational assessments of the Pacific and European networks, and the TS/SCI network managed by the Defense Intelligence Agency were conducted. The



- GIG-BE uses a government designed network management system, assembled from commercial hardware and software, and tested in a government facility.

## Mission

- Users in the intelligence community, combatant commands, and DoD employ GIG-BE to move critical information by providing virtually unlimited bandwidth.
- It provides secure communications for TS/SCI traffic and encrypts all outside the continental United States unclassified transmissions.
- It consolidates diverse DoD and Intelligence Community networks and leased circuits onto a single integrated, adaptable, backbone network.
- It serves Internet Protocol users, Defense Information System Network users, and transformational users with applications such as Internet Protocol version 6.
- Because it is the primary communications link between key fixed locations, GIG-BE must be survivable.

full-capability operational test and evaluation started in September 2005 and concluded in October 2005. The JITC published a final report in November 2005.

- The operational assessments employed traffic generators to evaluate the support for DoD communications protocols as well as latency, bit error rate, packet loss, and priority/precedence performance. The operational assessments exercised Continuity of Operations among the three collateral network operations centers (NOCs), and failover to backup paths whenever damage occurs to the primary network.

- The full-capability operational test and evaluation evaluates network management at the collateral and intelligence community NOCs, as well as live communication services with live user traffic at 20 of the 55 operational sites on the collateral network and simulated traffic on the intelligence community TS/SCI network.
- Operational testing has been done in accordance with the DOT&E approved Test and Evaluation Master Plan and test plans.

## Assessment

- GIG-BE is operationally effective in that it supports all approved DoD protocols; meets latency, packet loss, bit error rate, and priority/precedence standards; and carries all required types of operational traffic.
- GIG-BE is operationally suitable to support a limited number of users. Although progress continues to be made, some processes still must mature to support the full user population. These include the European NOC completing its ramp up to a full complement of operators, obtaining the full set of required spare parts, and replacing the interim configuration process currently being done manually by the automated Integrated Configuration Tracking System. None are high risk to a positive assessment.
- Through the operational assessment testing, GIG-BE was judged to be survivable because it has sufficient route diversity and successfully demonstrated Continuity of Operations in all three theaters, as well as on the optical and Internet

Protocol layers. Questions remain as to whether this level of survivability is sufficient as other key DoD networks transition onto the GIG-BE.

- More testing is needed for the TS/SCI network. The network and processes are mature in some areas and less mature in others. There was no final configuration of the network, management processes, or security fully represented in the test. The network remains to be integrated into the intelligence community methods for information assurance defense and configuration management, due to the necessary completion of an alternate NOC and successful demonstration of Continuity of Operations operations.
- The post-FOC transition consolidates many of DoD's legacy networks onto GIG-BE, making GIG-BE a more lucrative target than individual systems. As such, it warrants intensive follow-on information assurance evaluation.

## Recommendations

1. Develop follow-on evaluations for information assurance security and survivability, and mature TS/SCI operations to include Continuity of Operations actions with the TS/SCI network's alternate NOC.
2. Ensure that the Integrated Configuration Tracking System continues development and is fielded in a timely manner to ensure integration and configuration management tools are available to support effective scale up of operational traffic.